

An aerial photograph of a Norwegian fjord. The water is a deep blue, reflecting the sky. Steep, rocky mountains with patches of green moss and small trees surround the water. A small village with colorful houses and a church is visible on a peninsula. A winding road follows the coastline. The sun is low in the sky, casting a warm glow on the mountains.

Ephemeral Diffie-Hellman Over COSE (EDHOC)

draft-ietf-lake-edhoc-04

LAKE Interim, January 2021

Changes

Main changes from -03 to -04

- Outer encryption in message_2 defined as binary additive stream cipher, using (HKDF-)Expand
 - Essentially reversion to -02
- Specification of message_4
 - Optional to support
 - Key confirmation is mandatory
- Change normative text on cipher suits
 - Cipher suites 0 **and** 2 SHOULD be implemented
 - Constrained devices SHOULD implement 0 **or** 2
- Clarification of error messages
 - All error messages are fatal
- Review update of Section 1 (Introduction)

Open Issues

<input type="checkbox"/>	<input type="checkbox"/> 24 Open <input type="checkbox"/> 23 Closed	Author
<input type="checkbox"/>	Update acknowledgements. #59 opened 3 days ago by emanjon	
<input type="checkbox"/>	Length values when using the Exporter for OSCORE LAKE interim jan 2021 #58 opened 5 days ago by marco-tiloca-sics	
<input type="checkbox"/>	Passing information to the application LAKE interim jan 2021 #57 opened 5 days ago by marco-tiloca-sics	
<input type="checkbox"/>	Clarify decryption of CIPHERTEXT_2 LAKE interim jan 2021 #52 opened 13 days ago by marco-tiloca-sics	
<input type="checkbox"/>	Test vector #51 opened 15 days ago by fpalombini	
<input type="checkbox"/>	Add cipher suite with Wei25519 #50 opened on Dec 18, 2020 by emanjon	
<input type="checkbox"/>	Test vectors additions #47 opened on Dec 14, 2020 by fpalombini <input type="button" value="0 of 5"/>	
<input type="checkbox"/>	Test vectors not adhering to section 4.4.3 (cipher suite verification by the Responder) #44 opened on Dec 14, 2020 by TimothyClaeys	
<input type="checkbox"/>	Redundant Responder private key #43 opened on Dec 14, 2020 by TimothyClaeys	
<input type="checkbox"/>	Missing Responder private key in test vector. #42 opened on Dec 14, 2020 by TimothyClaeys	
<input type="checkbox"/>	Add guidelines for distinguishing received messages. Relates to #30. LAKE interim jan 2021 #39 opened on Dec 4, 2020 by marco-tiloca-sics	
<input type="checkbox"/>	How to do encryption without integrity in message_2 LAKE interim jan 2021 #34 opened on Nov 13, 2020 by emanjon	

<input type="checkbox"/>	Identifying a certificate with 'kid' by specified #32 opened on Nov 13, 2020 by emanjon
<input type="checkbox"/>	What exactly is ERR_MSG and how to distinguish a regular message from an error message LAKE interim jan 2021 #30 opened on Nov 11, 2020 by StefaniHri
<input type="checkbox"/>	Forward and backward secrecy #24 opened on Nov 6, 2020 by gselander
<input type="checkbox"/>	Agreement/negotiation of parameters/options #23 opened on Nov 6, 2020 by gselander
<input type="checkbox"/>	Rekeying of AEAD algorithms #20 opened on Nov 3, 2020 by emanjon
<input type="checkbox"/>	Optional message_4 for key confirmation LAKE interim jan 2021 #18 opened on Nov 2, 2020 by emanjon
<input type="checkbox"/>	Agreement of method #11 opened on Aug 1, 2020 by gselander
<input type="checkbox"/>	Injective agreement issue (was: G_IY in session key material) #10 opened on Aug 1, 2020 by gselander
<input type="checkbox"/>	Verification of intended peer #8 opened on Aug 1, 2020 by gselander
<input type="checkbox"/>	Clarify properties inferred from other crypto #6 opened on Aug 1, 2020 by gselander
<input type="checkbox"/>	Clarify assumptions regarding use of TEE #5 opened on Aug 1, 2020 by gselander
<input type="checkbox"/>	Self-contained specification #1 opened on Jul 7, 2020 by gselander

Closed Issues

- Shall we specify EDHOC in terms of KEM? (#17) → *No*
 - Mandatory to implement cipher suite (#22)
 - Use of SHA-512 in constrained IoT (#21)
 - Ciphersuites requiring multiple SHA (#2)
- *New normative text*
- Replace PSK ECDHE (#3) → *EDHOC-Rekey-FS()*
 - Need for resumption procedure? (#25) → *No*
 - Support of SHAKE and KMAC (#19) → *Done*
 - Register ciphersuites with high security (#35) → *Done*
 - Reference draft-mattsson-cose-cbor-cert-compress (#33) → *Done*
- + Editorial issues

ID encryption in message_2

- How to do encryption without integrity in message_2 (#34)
- Clarify decryption of CIPHERTEXT_2 (#52)

— Outer encryption of message_2 only needs protection from passive attackers.

1. Binary additive stream cipher. Key stream from (HKDF-)Expand function
2. Remove the tag from AEAD ciphertext. Only works when AEAD has a well-defined tag.
3. Associate an IND-CPA encryption alg with each AEAD. Requires table. (AES-CCM, AES-GCM -> AES-CTR, ChaCha20-Poly1305 -> ChaCha20)

— HKDF-Expand compared to AES-CTR

- Better confidentiality
- Slower for long plaintext, not an issue here

- Any objections to 1?

-02 & -04

-03

Candidate
for -03



THE CAPELLO E CAPOTE OF THE AZORES.
FROM A PHOTOGRAPH.

Optional message_4 1(2)

- **Optional message_4 for key confirmation (#18)**

- Last meeting conclusion: specify optional message_4 and some way to signal its use.
- New section 7.1 specifies message_4 and processing

```
message_4 = (  
  data_4,  
  MAC_4 : bstr,  
)
```

```
data_4 = (  
  ? C_1 : bstr_identifier,  
)
```

Compute an inner COSE_Encrypt0 ... :

- protected = h''
- external_aad = << TH_4 >>
- plaintext = h''

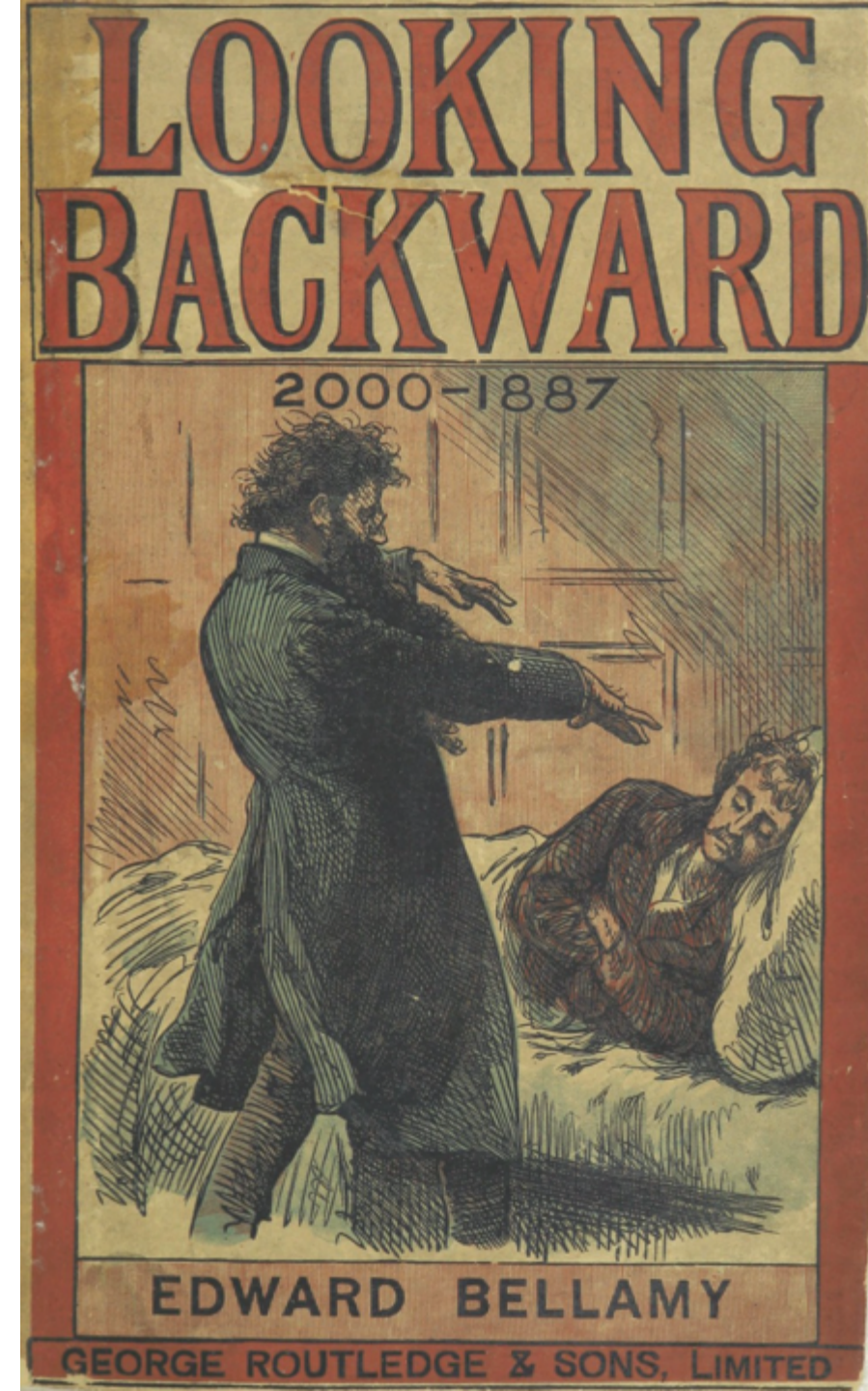
- Key for the MAC derived from the Exporter, using label "EDHOC_message_4_Key".
- No signalling → Key confirmation is instead mandatory
- Initiator expects protected application message, or message_4:
 - "In deployments where no protected application message is sent from the Responder to the Initiator, the Responder MUST send message_4."
- TBD: define action for Initiator that does not receive confirmation.
- **Comments?**

Optional message_4 2(2)

- Straightforward to specify Auxiliary Data for message_4. Not to be included in key derivation.
 - plaintext = AD_4
 - Rename MAC_4 → CIPHERTEXT_4
- **Shall we specify AD_4? Adds complexity, but only to message_4 which is optional.**

Forward and backward secrecy

- Forward and backward secrecy (#24)
- Related to
 - AEAD rekeying (#20) → *TBD in CoRE*
 - TEE (#5) → *Updated security consideration*
- Discussed at LAKE interim Dec. 2020.
- <https://datatracker.ietf.org/doc/minutes-interim-2020-lake-04-202012181600/>
- “Working assumption is either do full EDHOC exchange, or hash-based forward secrecy which requires no asymmetric operations. No formal ratcheting.”
- Renamed in -04: EHDHC-Rekey-FS(nonce)
 - $PRK_{4x3m} = \text{Extract}(["TH_4", \text{nonce}], PRK_{4x3m})$
- (To be followed by a call of EDHOC-Exporter for fresh keys)
- Comments?



Error Message Diagnostics

- **What exactly is ERR_MSG (#30)**

```
error = (  
  ? C_x : bstr_identifiser,  
  DIAG_MSG : tstr,  
  ? SUITES_R : [ supported : 2* suite ] / suite,  
)
```

- Changed name ERR_MSG → DIAG_MSG
 - mandatory and characteristic for error messages
 - human-readable diagnostic message in English
- Intended for software engineers during debugging
- SHOULD be provided to the calling application
- SHOULD be logged
-
- **What diagnostic messages needs to be standardized, if any?**



Distinguish Messages

- How to distinguish a regular message from an error message (#30)
- Add guidelines for distinguishing received messages (#39)

- error int / bstr, tstr
- message_1 int, [] / int
- message_2 int / bstr, bstr
- message_3 int / bstr, bstr

- CBOR items uniquely identify error from non-error message
- **What kind of implementation guidance needed?**



Length values when using the Exporter for OSCORE (#58)

- Request: state that the two values for the 'length' parameter are just default values and that it is allow for peers to agree out-of-band.
 - Master Secret = EDHOC-Exporter("OSCORE Master Secret", length)
 - Master Salt = EDHOC-Exporter("OSCORE Master Salt", 8)
- For master secret, length is the key length (in bytes) of the application AEAD Algorithm.
- **Comments?**

Passing information to the application (#57)

- Request: Be explicit about what should be passed to the application if a verification step fail and the protocol is discontinued.
- Diagnostic error message, which should be logged.
- Anything else?
- **Comments?**

More ways to identify certificates ('kid', 'c5u', c5t')

- **Reference draft-mattsson-cose-cbor-cert-compress (#33) → Done**
- **Identifying a certificate with 'kid' (#32) → TBD**
- Currently the specification assumes that certificates are identified with 'x5t' or 'x5u' and RPK are identified with a 'kid'.
- COSE WG is currently exploring "CBOR Certificates" specifying 'c5t', 'c5u' → *Referenced in -04*

Test Vectors

- **Test vectors additions (#47)**
- **Test vector (#51)**
- Obsolete PSK test vectors → *Done*
- Add TH4 output
- Add exporter and exporter outputs to test vectors
- Add certificates to test vectors
 - Natively signed CBOR certificates (type 0)
 - Later: ASN.1/DER encoded (type 1)
- Add ciphersuites 2 and 3 to test vectors
- **The change of label in key derivation in -04 makes test vectors in the draft obsolete**
- **Plan to have updated test vectors for IETF 110**
- **Test vectors with real certificates, more cipher suites, error messages & Rekey-FS will follow**



Recent Issues

- **COSE_Key content constrained according to EDHOC (#62)**

" For COSE_Keys of type EC2 the CBOR map SHALL only include the parameters 1 (kty), -1 (crv), -2 (x-coordinate), and -3 (y-coordinate). "

- **Change message_1 format (#61)**

Can both message_3 and message_1 be started with C_R that helps the parsing and makes a distinction between the two messages.

In message_1 C_R = h" means that C_R is to be calculated by Receiver.

Otherwise C_R serves to determine it is a new connection (message_1) or an existing ongoing connection (message_3).

- **Test vectors comments from Peter (#60)**

WANTED

CONTINUE ISSUE
DISCUSSION ON
GITHUB

MORE REVIEWS

PARTICIPATE
IN INTEROP